

METHOD AND APPARATUS FOR PROTECTING A WEB SERVER AGAINST VANDALS ATTACKS WITHOUT RESTRICTING LEGITIMATE ACCESS

ABSTRACT

5 An intrusion detection security system (IDSS) guards a server against vandals' attacks such as denial of service, distributed denial of service, and common gateway interface attacks. An incoming source address is compared with the contents of a database of privileged addresses. If the incoming address is present in the database, the IDSS instructs protective equipment such as a firewall or router to allow the incoming message to pass to the web server despite any ongoing attack, thus allowing messages from customers or suppliers, for example, through. Otherwise, the IDSS checks a database of blocked addresses. When the incoming address is absent, the IDSS writes the address to the database of blocked addresses and instructs the protective equipment to block subsequent messages from the incoming address.